УДК 004.056

ОСНОВНЫЕ ПОЛОЖЕНИЯ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИЕРАРХИЧЕСКИХ РАСПРЕДЕЛЕННЫХ СИСТЕМ

К.Н. Филькин

Томский государственный университет систем управления и радиоэлектроники.
E-mail: fkn@kibevs.tusur.ru

Представлены основные положения модели информационной безопасности иерархических распределенных систем. Рассмотрены основные проблемы данных систем, дано определение основных составляющих элементов модели, уровней доверия, свойств распределенности и иерархичности сегментов системы, политики верификации времени.

Введение

Одним из основных направлений информационной безопасности является создание формальных моделей информационной безопасности, называемых также моделями разграничения доступа. Под моделью информационной безопасности понимают формально описанную политику безопасности – совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности [1].

Среди множества моделей безопасности можно выделить основные типы моделей: дискреционные модели, мандатные модели, модели с ролевым разграничением доступа.

Дискреционные модели безопасности – модели, основанные на дискреционном управлении доступом (Discretionary Access Control), которое определяется двумя свойствами:

1) все субъекты и объекты идентифицированы;
2) права доступа субъектов к объектам системы определяются на основании некоторого внешнего по отношению к системе правила.

Основным элементом моделей дискреционного разграничения доступа является матрица доступов. Классическими моделями данного типа является модель Харрисона-Руззо-Ульмана [2] и модель Take-Grant [3]. Дискреционные модели при условии своей очевидной простоты обладают рядом недостатков, основными среди которых являются незащищенность от атаки «троянский конь», недоказуемость безопасности всех состояний системы. Несмотря на недостатки, данные модели следует использовать в комбинации с другими моделями.

Мандатные модели основаны на мандатном разграничении доступа (Mandatory Access Control), представляющем собой совокупность правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов. Характерный пример – модель Белла-ЛаПадулы [4]. В данной модели анализируются условия, при выполнении которых в компьютерной системе невозможно возникновение информационных потоков от объектов с большим уровнем конфиденциальности к объектам с меньшим уровнем конфиденциальности. Для этого вводится решетка уровней конфиденциальности, которым сопоставляются субъекты и объекты. Авторы модели предложили теорему, которая утверждает, что система с безопасным начальным состоянием является безопасной тогда и только тогда, когда при любом переходе системы из одного состояния в другое не возникает никаких новых и не сохраняется никаких старых отношений доступа, которые будут небезопасны по отношению к функции уровня безопасности нового состояния. В реальности, данная модель используется только в системах, обрабатывающих классифицированную информацию и применяется только в отношении ограниченного множества субъектов и объектов.

Модели с ролевым разграничением доступа (Role-Based Access Control) [5] представляют собой развитие политики дискреционного разграничения доступа. Права доступа субъектов системы к объектам группируются с учетом специфики их применения, образуя роли. При этом правила данной модели являются более гибкими, чем правила мандатной модели, построенные на основе жестко определенной решетки ценности информации. В ролевой модели классическое понятие «субъект» заменяется понятиями «пользователь» и «роль». Пользователь – это человек, работающий с системой и выполняющий определенные служебные обязанности. Роль – это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логически связанный набор полномочий, необходимый для осуществления определенной деятельности. При использовании ролевой политики управление доступом осуществляется в две стадии: во-первых, для каждой роли указывается набор полномочий, представляющих набор прав доступа к объектам, и, во-вторых, каждому пользователю назначается список доступных ему ролей.

В настоящей работе рассматривается особый класс информационных систем – иерархические распределенные системы (ИРС). Данный класс систем характеризуется особыми свойствами и связанными с ними проблемами:

1. Большое число узлов сети, в том числе серверов и рабочих станций.
2. Логическая и физическая распределенность различных частей системы.
3. Сосуществование локальной и глобальной сетей.

4. Проблема верификации времени между различными сегментами.
5. Доверенная вычислительная среда, режимы доверия.
6. Сложность создания и верификации политики безопасности, регламентирующей разделения доступа пользователей к объектам.

Общие положения и основные понятия

Модель информационной безопасности ИРС содержит несколько составных частей, предназначенных для разрешения указанных выше проблем.

1. Свойство распределенности сегментов ИРС.
2. Свойство иерархичности сегментов ИРС.
3. Введение групп и контейнеров для упорядочивания множеств субъектов и объектов.
4. Описание доверительных отношений сегментов.
5. Политика верификации времени.
6. Описание безопасного состояния и безопасных переходов.
7. Взаимодействие с внешними системами.
8. Описания языка построения политики безопасности.

В данной статье приводится описание лишь некоторых данных свойств. Рассмотрим основные понятия, на которых строится модель безопасности ИРС, и введем математическое описание для основных элементов модели. Основные свойства рассматриваемого класса систем – распределенность и иерархичность.

Определение 1. Локальным сегментом в распределенной информационной системе называется часть распределенной системы, представляющая собой совокупность подмножества объектов доступа, подмножества пользователей, физических объектов с отдельной политикой информационной безопасности.

$L = \{L_i \mid i=1...N\}$ – множество локальных сегментов распределенной системы.

$(E, \leq)$ – решетка уровней иерархии системы.

Определение 2. Локальной политикой безопасности называется политика безопасности, действующая в локальном сегменте.

Локальная политика безопасности реализуется локальным монитором безопасности, который обеспечивает выполнение всех функций информационной безопасности.

Определение 3. Локальным монитором безопасности называется системный субъект, реализующий политику разграничения доступа в локальном сегменте распределенной системы, регламентирующую доступы внутри данного сегмента, а также доступы к элементам данного сегмента из других локальных сегментов.

Определение 4. Глобальной политикой безопасности называется политика безопасности, действующая во всей системе, регламентирующая правила, взаимодействия отдельных локальных сегментов.

Как правило, глобальная политика безопасности состоит из локальных политик и общей политики их урегулирования.

Определение 5. Глобальным монитором безопасности называется субъект, отслеживающий любые потоки между локальными сегментами, разрешая потоки из фиксированного подмножества разрешенных доступов.

Определение 6. Объект – это одноуровневый блок информации. Он не может содержать других объектов.

Обозначим O – множество информационных объектов, которое состоит из подмножеств объектов каждого сегмента, то есть:

$O = \bigcup_{i=1}^{N} O^i = \bigcup_{i=1}^{N}\bigcup_{j=1}^{M} o_j^i$, где $O^i=\{o_j^i \mid j=1...M\}$ – множество объектов локального сегмента L_i.

Определение 7. Контейнер – это многоуровневая информационная структура. Контейнер может содержать другие объекты и другие контейнеры.

C – множество контейнеров.

Определение 8. Сущность – это объект или контейнер.

$SU=O\cup C$ – множество сущностей.

Также обозначим множество физических объектов системы V – вычислительных установок (рабочие станции, серверы), принтеров, коммуникационного оборудования и т. п.

Выделим из множества субъектов S множество всех пользователей $U\in S$, которое состоит из подмножеств пользователей каждого сегмента, то есть:

$U = \bigcup_{i=1}^{N} U^i = \bigcup_{i=1}^{N}\bigcup_{j=1}^{M} u_j^i$, где $U^i=\{u_j^i \mid j=1...M\}$ – множество пользователей локального сегмента L_i.

Определение 9. Группа – это совокупность пользователей, объединенных едиными правами доступа к объектам и/или едиными привилегиями (полномочиями) выполнения процедур обработки данных в рамках определенных функциональных обязанностей.

Обозначим G – множество групп пользователей.

Определение 10. Юнит – это отдельный пользователь или группа.

Обозначим множество юнитов $UN=U\cup G$.

Определение 11. Роль пользователя – совокупность прав пользователя, определяемая характером выполняемых им действий в системе.

Обозначим через R множество ролей пользователей и P – прав доступов к объектам системы.

Определение 12. Иерархией ролей называется заданное на множестве ролей отношение частичного порядка «≤».

Отношение частичного порядка на множестве ролей не обязательно задает на нем решетку.

Как было отмечено выше, группы – это множества, содержащие пользователей и другие группы. Можно сказать, что субъект s является членом группы G непосредственно, если он определен как член группы G, и косвенно, если существует последовательность $G_1, G_2, ..., G_n$, $n > 1$, так что G_i непосредственный член G_{i+1} для i=1, ..., n–1. Единственным ограничением на членство в группе является ацикличность, т. е., если G_i член G_j, то G_j не может быть членом G_i. Членство в группе может быть представлено в виде графа, узлы которого – индивидуальные пользователи или группы, а дуги отражают членство. Данный граф является иерархией групп.

Основное отличие между ролями и группами состоит в том, что первые могут быть активированы и деактивированы пользователями по их желанию, тогда как ограничения, накладываемые группами, применяются всегда. Специфика ИРС дает еще одно отличительное свойство, которое характеризует особенность групп в рамках концепции данных систем. Группы пользователей в ИРС связаны с их иерархической структурой, тем самым на множестве групп задается отношение частичного порядка «≤».

Уровни доверия

На множестве L локальных сегментов системы определяется частичный нестрогий порядок, устанавливающий систему доверительных отношений.

f_{LL} : $L \times L$ – отношение, определяющее приоритет доверия одних локальных сегментов по отношению к другим и задающее оператор доминирования «≤», такое что:

1. Если для L_i, $L_j \in L$ и L_i «=» L_j, то между данными локальными сегментами установлены отношения двустороннего доверия (т. е. возможны удаленные доступы юнитов локального сегмента L_i к сущностям сегмента L_j, и наоборот, юнитов L_i к сущностям L_j).
2. Если для L_i, $L_j \in L$ и L_i «≠» L_j, то отношения доверия между данными локальными сегментами не установлены (т. е. невозможны удаленные доступы юнитов сегмента L_i к сущностям сегмента L_j и удаленные доступы юнитов L_i к сущностям L_j).
3. Если для L_i, $L_j \in L$ и L_i «<» L_j, то между данными локальными сегментами установлены отношения одностороннего доверия (т. е. возможны удаленные доступы пользователей сегмента L_i к сущностям сегмента L_j, но удаленные доступы пользователей L_i к сущностям L_j невозможны).

Следует также отметить, что среди всех данных вариантов для ИРС будет превалировать третий случай – отношений одностороннего доверия, которые характерны для иерархических структур.

Политика верификации времени

Рассмотрим теперь верификацию времени между локальными сегментами.

Механизм проверки установленного времени внутри между различными компонентами ИРС необходим для устранения следующих угроз:

- реализация атаки подмены времени у передаваемых данных (преднамеренная угроза);
- невозможность доступа к информации вследствие необнаруженного несоответствия установленного времени на различных сегментах (непреднамеренная угроза).

Данные угрозы особенно критичны, в том числе, для следующих случаев:

- при использовании в распределенных системах средств криптографической защиты информации и средств электронно-цифровой подписи;
- при построении защищенных частных виртуальных сетей (VPN);
- при передаче особо важной информации, к которой предъявляются особые требования по срокам доставке.

В основу учета уставленного времени положен следующий принцип. Каждому локальному сегменту ставится в соответствие некоторая временная зона. В каждом локальном сегменте локальным монитором безопасности ведется учет установленного времени на отдельных вычислительных установках. Также при межсегментных информационных потоках проводится верификация установленного времени субъекта, осуществляющего удаленный доступ.

Введем следующее обозначение:

W – множество временны́х зон (например, они могут быть сопоставимы со световыми поясами).

f_{LW}: $L \times W$ – отношение, ставящее в соответствие каждому локальному сегменту временную зону.

Сделаем следующее предположение: каждому локальному сегменту L_i ставится в соответствие единственная временная зона w_j.

В каждом локальном сегменте $L_i \in L$ на каждом вычислительном ресурсе $v_j \in V$ из множества субъектов выделяется особый системный субъект $s_time_j^i \in S$, ассоциированный со временем.

Локальный монитор безопасности производит проверку (аутентификацию) субъектов, ассоциированных со временем, сопоставляя информацию с временной зоной локального сегмента. Для этого вводится предикат:

$local_audit_time(v_j)$,

возвращающий «*True*» при условии совпадения времени на вычислительном ресурсе времени, принятому в локальном сегменте, и «*False*» в ином случае.

При возникновении потоков между различными сегментами в процедуру начальной аутентификации включается проверка предиката

$global_audit_time(L_1, L_2)$,

который контролирует верность соответствия элементов локальных сегментов, участвующих в удаленном доступе, временным зонам данных сегментов. Данная проверка производится глобальным монитором безопасности.

Выводы

Рассмотрены вопросы безопасности иерархических распределенных систем. На основании особенностей иерархических распределенных систем разработана новая модель информационной безопасности, учитывающая многокомпонентность, распределенность и многоуровневость. Сформулирован базис основных понятий и положений, на основе которых строится данная модель. Описаны система доверительных отношений и политика верификации времени.

СПИСОК ЛИТЕРАТУРЫ

1. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
2. Harrison M., Ruzzo W., Ullman J. Protection in operating systems // Communication of ACM. – 1976. – № 19(8). – P. 461–471.
3. Jones A., Lipton R., Snyder L. A Linear Time Algorithm for Deciding Security // On the Foundations of Computer Science: Proc. 17th Annual Symp. – Houston, 1976. – P. 33–41.
4. Bell D.E., LaPadula L.J. Secure Computer Systems: Unified Exposition and Multics Interpretation. – Belford, Mas.: MITRE Corp., 1976. – 129 p.
5. Sandhu R. Coynek E., Feinsteink H., Youman C. Role-Based Access Control // IEEE Computer. – 1996. – № 29(2). – P. 38–47.
6. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во Урал. ун-та, 2003. – 328 с.

УДК 004.75